



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,377	12/20/1999	YURIJ ANDRIJ BARANSKY	Y0999-558	3573
7590	08/25/2005		EXAMINER	
ANNE V. DOUGHERTY, ESQ. 3173 Cedar Road Yorktown Heights, NY 10598			NALVEN, ANDREW L	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/468,377	BARANSKY ET AL.
Examiner	Art Unit	
	Andrew L. Nalven	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 07 June 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-20 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 20 December 1999 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____

DETAILED ACTION

1. Claims 1-20 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-17 have been considered but are not persuasive.

3. Applicant has argued on page 17 against Examiner's assertion that the knowledge of a key cannot be claimed. Examiner continues to maintain that the knowledge of a key to only the content provider or to the client is not a property of the key. As stated in the prior office action, it is impossible to claim such a limitation because it cannot be proven. Further, it is unclear to the Examiner how such a claim can be made because it appears that keys cited as being only known to a particular entity are sent to other entities (see 35 USC 112 rejections set forth below). Hence, for the remainder of this office action, the limitations directed towards the knowledge of a key to a particular party have not been given patentable weight.

4. Applicant has argued on page 22 that the Thomlinson reference fails to teach a content provider by asserting that Thomlinson teaches a different security arrangement. Examiner contends the claimed limitations only show the steps involved between a content provider and a user in establishing encryption and authentication processes. The service provider defined by the present invention does not participate in the claimed processes. The Thomlinson reference also teaches only two entities (user and

provider) involved with establishing encryption and authentication processes. Thus, Examiner contends that the security arrangement of Thomlinson is the same as the arrangement of the present invention.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 9, 14 and 17 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: the sending of the encrypted g^b to the client machine.

7. Claims 1, 5 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. With regards to claims 1, 5, 12-13, 15-16, the cited claims provide the step of "decrypting said encrypted second key using said one-time password" (see step e). Step b defines the second key as being encrypted by a one-time password and said first key. It is unclear to the examiner how the encrypted second key may be decrypted by using only the one time password and not also using the first key. It is also unclear to

the Examiner how the decryption of the second key would take place at the client without revealing the first key to the client.

9. With regards to claims 9, 14, and 17, the cited claims contain the following limitation as part of step e, "wherein an encryption key Kab... uses g^{ab}." Examiner is unclear as to how an encryption key uses another encryption key. Further, the cited claims state only the content provider knows the value of b (see element a). The cited claims later stat that the client decrypts the encrypted g^b. Since the client is in possession of the value of g, it is unclear to the examiner how the client would not know of the value of b as well. A client in possession of the value of g and g^b would be able to calculate the value of b.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 3-4, 7-8, 12, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 in view of Aziz US Patent No. 5,604,803. Thomlinson a system for cryptographic protection of core data secrets. Aziz teaches a method for secure remote authentication in a public network.

12. With regards to claims 1,12, and 15, Thomlinson teaches the generating of a first key (Thomlinson, column 9 lines 20-22, master key), the encrypting of a second key using the first key and an encryption algorithm (Thomlinson, column 9 lines 20-22, item key encrypted by master key), decrypting the second key using the first key when the user desires access to data (Thomlinson, column 10 lines 5-13, decrypt item key using master key), the storing of an encrypted second key on the client machine (Thomlinson, column 9 line 63 – column 10 line 4), and accessing the data using the second key (Thomlinson, column 10 lines 15-16). Thomlinson lacks a reference to the use of a one-time password. Aziz teaches the use of a one-time password (Aziz, column 6 lines 61-64). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Aziz's method of using one-time passwords with Mi's access control system because it offers the advantage of reducing the likelihood of an unauthorized user gaining access to user passwords (Aziz, column 2 lines 1-13).

13. With regards to claims 3 and 7, Thomlinson as modified teaches the one-time password being a unique user identifier and the one time password being transmitted out of band (Aziz, column 2 lines 45-60).

14. With regards to claims 4 and 8, Thomlinson as modified teaches a second key being required in an algorithm that generates a session key used to decrypt data (Thomlinson, column 10 lines 11-16).

15. Claims 2, 5-6, 13, 16, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535 and Aziz US Patent No.

5,604,803, as applied to claims 1, 12, and 15 above, and in further view of Mi et al US

Patent No. 6,418,472.

16. With regards to claims 2 and 6, Thomlinson as modified fails to teach the step of transmitting the identity of the client machine to the content provider. Mi teaches the step of transmitting the identity of the client machine to the content provider to authenticate that the user is using the client machine thereby permitting data to be accessed only on the client machine (Mi, column 8 lines 32-46). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Mi's method of transmitting a client's identity with Thomlinson as modified because it offers the advantage of allowing the identification of a platform or device employed by the user prior to granting access to an object (Mi, column 1 line 69 – column 2 line 2).

17. With regards to claims 5, 13 and 16, Thomlinson as modified teaches everything described above and the use of a separate user supplied password (Thomlinson, column 10 lines 5-9), but fails to teach the user accessing a web page of said content provider, downloading an applet from said content provider to said client machine. Mi teaches the user accessing a web page of said content provider, downloading an applet from said content provider to said client machine (Mi, column 5 lines 4-21, column 6 lines 15-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Mi's applet procedure with Thomlinson as modified because it offers the advantage of providing a tamper resistant user friendly

method of authentication that helps identify a user (Mi, column 1 line 61 – column 2 line 5).

18. With regards to claims 18-19, Thomlinson as modified teaches authenticating the user to said content provider based on said stored mapping (Mi, column 4 lines 45-52, column 5 lines 43-60), generating a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, master key), encrypting a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, item key encrypted by master key), encrypting said additional data with said new encryption key (Thomlinson, column 9 lines 13-19), and transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key (Thomlinson, column 10 lines 15-16).

19. Claims 9, 14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389 in view of Aziz US Patent No. 5,604,803, and Jablon US Patent No. 6,226,383. Jablon describes cryptographic methods for remote authentication.

20. With regards to claims 9, 14, and 17, Thomlinson teaches the generating of a first key (Thomlinson, column 9 lines 20-22, master key), the encrypting of a second key using the first key and an encryption algorithm (Thomlinson, column 9 lines 20-22, item key encrypted by master key), decrypting the second key using the first key when the user desires access to data (Thomlinson, column 10 lines 5-13, decrypt item key using

master key), the storing of an encrypted second key on the client machine (Thomlinson, column 9 line 63 – column 10 line 4), and accessing the data using the second key (Thomlinson, column 10 lines 15-16). Thomlinson lacks a reference to the use of a one-time password, the sending of g^a to the client machine, generating g^b , encrypting g^b , and calculating $g^{(a*b)}$ as part of the authentication procedure. Aziz teaches the use of a one-time password (Aziz, column 6 lines 61-64). Jablon teaches a procedure called Hidden-Password Validation that includes the sending of g^a to the client machine (Jablon, column 7 lines 16-23), generating g^b (Jablon, column 7 lines 23-26), encrypting g^b (Jablon, column 7 lines 23-26) g^b is exchanged using Diffie-Hellman encryption), and calculating $g^{(a*b)}$ (Jablon, column 7 lines 25-27) as part of the authentication procedure. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Aziz's method of using one-time passwords and Jablon's exchange procedures with Thomlinson's system because it would offer the advantage of reducing the likelihood of an unauthorized user gaining access to user passwords (Aziz, column 2 lines 1-13) and because it would help reduce the vulnerability of the password if a host computer's password database is exposed (Jablon, column 20 lines 17-20).

21. Claims 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al US Patent No. 6,389,535, Aziz US Patent No. 5,604,803, and Jablon US Patent No. 6,226,383, as applied to claim 9 above, and in further view of Mi et al US Patent No. 6,418,472.

22. With regards to claim 10, Thomlinson as modified fails to teach the step of transmitting the identity of the client machine to the content provider. Mi teaches the step of transmitting the identity of the client machine to the content provider to authenticate that the user is using the client machine thereby permitting data to be accessed only on the client machine (Mi, column 8 lines 32-46). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Mi's method of transmitting a client's identity with Thomlinson as modified because it offers the advantage of allowing the identification of a platform or device employed by the user prior to granting access to an object (Mi, column 1 line 69 – column 2 line 2).

23. With regards to claim 20, Thomlinson as modified teaches authenticating the user to said content provider based on said stored mapping (Mi, column 4 lines 45-52, column 5 lines 43-60), generating a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, master key), encrypting a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, item key encrypted by master key), encrypting said additional data with said new encryption key (Thomlinson, column 9 lines 13-19), and transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key (Thomlinson, column 10 lines 15-16).

24. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable Thomlinson et al US Patent No. 6,389,535, Aziz US Patent No. 5,604,803, and Jablon US Patent No. 6,226,383 as applied to claim 9 above, and further in view of Schneier Applied Cryptography.

25. With regards to claim 11, Thomlinson as modified, lacks a reference to a MAC authentication procedure. Schneier describes the one-way hash function termed a MAC that is used to verify authenticity (Page 455, Section 18.14). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's MAC authentication on g^{a^*b} to authenticate the server to the client because it provides a verification method that is reliant on having the same key. Both client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security since it is a one-way function (Page 455, Section 18.14).

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalyen

